CROSS REFERENCE TO RELATED APPLICATIONS

This application takes priority under 35 U.S.C. §119(e) of U.S. Patent Application No 60/481,313 filed August 29, 2003 (Attorney Docket No.: TRNDP009P) naming Liang et al. as inventor(s) entitled "VIRUS MONITOR AND METHODS OF USE THEREOF" which is also incorporated herein by reference for all purposes. This application is also related to the following co-pending U.S. Patent applications, which are filed concurrently with this application and each of which are herein incorporated by reference, (i) U.S. Patent Application No. **10/684,330** (Attorney Docket No.: TRNDP009), entitled "VIRUS MONITOR AND METHODS OF USE THEREOF" naming Liang et al as inventors; (ii) U.S. Patent Application No. **10/683,528** (Attorney Docket No.: TRNDP010), entitled "AUTOMATIC REGISTRATION OF A VIRUS/WORM MONITOR IN A DISTRIBUTED NETWORK" naming Liang et al as inventors; (iii) U.S. Patent Application No. **10/683,873**, (Attorney Docket No.: TRNDP014), entitled "NETWORK ISOLATION TECHNIQUES SUITABLE FOR VIRUS PROTECTION", naming Liang et al as inventors; and (iv) U.S. Patent Application No. **10/683,874** (Attorney Docket No.: TRNDP012), entitled "ANTI-VIRUS SECURITY POLICY ENFORCEMENT", naming Liang et al as inventors; (v) U.S. Patent Application No. **10/683,579** (Attorney Docket No.: TRNDP011), entitled "NETWOKR TRAFFIC MANAGEMENT BY A VIRUS/WORM MONITOR IN A DISTRIBUTED NETWORK", naming Liang et al as inventors; and (vi) U.S. Patent Application No. **10/683,554** (Attorney Docket No.: TRNDP013), entitled "INNOCULATION OF COMPUTING DEVICES AGAINST A SELECTED COMPUTER VIRUS", naming Liang et al as inventors.

Please replace paragraph [0022] with the following amended paragraph:

[0022] In addition to providing scalability, the tiered architecture of network 100 provides for topologically advantageous positioning of the network virus monitor 102. For example, in the instant case, virus monitor 102 is placed between the tier 2 switch ~~122~~ **120** and the lower level tier 3 switch ~~124~~ **122** to which the various client devices 104 – 116 are coupled. In this way, all network traffic between the tier 2 switch (which may be coupled directly to the Internet backbone, for example) and any of the tier 3 switches can be monitored by the virus monitors 102 at a point prior to any of the client devices. By providing a bulwark against a potential virus attack, the virus monitors 102 provide a focal point for virus detection, virus outbreak prevention, and, if needed, virus outbreak cleanup and restoration that, in turn, effectively protect the various client devices from the attacking virus. It should be noted, that a docking port 125 can be included in network 100 arranged to accept temporary, or visitor, client devices.

Please replace paragraph [0027] with the following amended paragraph:

[0027] In addition to providing scalability, the tiered architecture of network 100 provides for topologically advantageous positioning of the network virus monitor 102. For example, in the instant case, virus monitor 102 is placed between the tier 2 switch 122 and the lower level tier 3 switch ~~124~~ to which the various client devices 104 – 116 are coupled. In this way, all network traffic between the tier 2 switch (which may be coupled directly to the Internet backbone, for example) and any of the tier 3 switches can be monitored by the virus monitors 102 at a point prior to any of the client devices. By providing a bulwark against a potential

virus attack, the virus monitors 102 provide a focal point for virus detection, virus outbreak prevention, and, if needed, virus outbreak cleanup and restoration that, in turn, effectively protect the various client devices from the attacking virus. It should be noted, that a docking port ~~125~~ can be included in network 100 arranged to accept temporary, or visitor, client devices.

Please replace paragraph [0038] with the following amended paragraph:

[0038] In the case where virus monitor 102 has detected a possible virus in one or more of the data packets (or in the case where a potential intruder attack is underway), virus monitor 102 generates an event flag. This event flag provides information based upon the detected virus using both the rules set 136 and the OPP file 135 as well as any other data deemed useful. Typically, the event flag is passed directly to the controller 126 which may, in some cases, forward the event flag to the server 138 for further analysis and/or disposition of any remedial actions, if any. This collaborative nature of the inventive virus monitoring system is well documented and described in co-pending U.S. Patent Application No. **10/411,665**, Attorney Docket No. 87152491-002027 entitled, "MULTILEVEL VIRUS OUTBREAK ALERT BASED ON COLLABORATIVE BEHAVIOR" by Liang et al filed **April 10, 2003** which is incorporated by reference herein in its entirety for all purposes.

Please replace paragraph [0039] with the following amended paragraph:

[0039] In some cases, the event flag represents a potential threat so severe that the operation mode of virus monitor 102 is immediately changed from the standby mode to what is referred to as the inline mode without intervention from

the controller 126 as shown in FIG. 5. In the inline mode, all data packets in the traffic flow T1 are analyzed without copying such that those data packets determined to be (or suspected of being) infected are not allowed to pass back into the traffic flow (in this case T1 is greater than T2). In this the virus is blocked from passing to and throughout network 100. In other instances where the event itself does not trigger virus monitor 102 to change operations mode to the inline mode, a mode change command ~~506~~ **502** from ~~either~~ the controller 126 or **a mode change command 504 from** the server 128 is used to trigger the mode change. In this way, the inventive anti-virus system has the added advantage of delegating authority to the virus monitors in those situations where speed is of the essence to contain a potential viral outbreak. On the other hand, in those cases where the threat is less clear, or further analysis is required, the onus of determining the threat potential and execution of a defense plan can be focused in higher level analysis engines (such as a system administrator, for example) thereby reducing false alarms and unnecessary system shutdowns.

Please replace paragraph [0041] with the following amended paragraph:

[0041] Therefore, each of the virus monitors 102 that have detected a virus or viruses in the associated traffic flow will dispatch a corresponding event report to the associated controller 126. The various controllers, in turn, will forward the various event reports to the server 128 where they will be collated and analyzed in order to determine if a virus warning ~~508~~ **506** should be generated. In the case where a virus warning is generated, the virus warning 506 is dispatched to those controllers 126 that the server 128 has determined to be most likely affected by the virus outbreak. In this way, any system administrator(s) can review the current

state of network 100 and be apprised of the potential threat for the system as a whole or for selected segments as might be considered important.